REMARKS

After entry of the foregoing amendment, claims 52-80 are pending in the application. Claims 73-80 are newly added.

New claims 75-80 are renumbered counterparts of independent claims submitted in the present case with an Amendment dated November 8, 2006. Those claims were withdrawn from consideration as directed to a non-elected invention (January, 2007 Action). However, since that Amendment was deemed "non-responsive" to the previous Action, it is not clear if the claims were ever formally entered in the present application.

So as to provide an unambiguous record, the claims are re-presented with this RCE application. They may again be found to be restrictable, for the same reasons detailed in the January, 2007 Action.

Applicant has amended claims 59 and 65, per the Examiner's suggestion, to overcome the § 112 rejections.

Claims 52-65 and 72 stand rejected as unpatentable over Reeds (5,203,902) in view of Hopper (3,406,344).

Reeds concerns an arrangement by which "secret data" can be shared between a cell phone handset and a local cell base station, for authentication and encryption purposes.

In his Background discussion Reeds notes that various authentication arrangements are known, e.g., using private keys and public/private key pairs, and that same have been used to validate a cell phone transaction at the time a call is made. However, Reeds explains that such arrangements are unsatisfactory because the back-and-forth protocols associated with key exchange and verification are too slow for consumer acceptance. Waiting seconds to get a dial tone is generally intolerable (*c.f.*, col. 2, lines 8-15).

Reeds' invention addresses this authentication delay problem by conducting authentication infrequently, i.e., only when a handset first enters a local base station's coverage area (*c.f.*, col. 3, lines 31-36). Much of the back-and-forth of prior art

techniques is thus obviated, because both the handset and the local base station already share a "secret" that enables them to communicate securely.

At the outset (e.g., at the time the customer's account is established), the handset is programmed with a phone number (MIN1), an area code (MIN2), and its own secret (A-key). Additionally, the handset was hardwired with an electronic serial number (ESN).

When the handset is first initialized, a processor within the handset's home cell service area (home CGSA) sends a random sequence (RANDSSD) to the handset, with a directive to create a SSD. The handset responds by concatenating its ESN, its A-key, and the RANDSSD sequence, and applying the Jumble digital signature process. (Col. 4, lines 47-55; col. 6, lines 3-11; Fig. 4).

The handset's home CGSA knows the handset's ESN and A-key, so it can perform the same calculation to independently compute the SSD (col. 6, lines 24-33).

The shared secret resulting from this process has two parts, SSD-A and SSD-B. The former is used to support handset authentication, while the second is used to encrypt the voice signal (col. 6, lines 12-16).

Reed also details a verification procedure to check that this common secret is, in fact, shared (col. 6, lines 34-60).

When the initialized handset thereafter enters a new cell coverage area, a registration process occurs – typically only once.

During this handset registration process, the handset receives a RAND sequence broadcasted by the local base station, and replies by sending the phone's phone number (MIN1), area code (MIN2), and serial number (ESN) in plaintext, as well as a hashed authentication string. This hashed authentication string is formed by concatenating RAND + ESN + MIN1 + SSD-A, and applying the Jumble procedure (col. 7, lines 21-34).

The local base station knows all of the foregoing information, except the handset's SSD-A (col. 7, lines 41-46). But from the handset's area code and phone number (MIN2 + MIN1), the local base station can lookup the handset's home CGSA, and it passes a request to the home CGSA for the SSD information – providing data known to the local base station, *i.e.,* the handset phone number, its ESN sequence, the

RAND sequence it issued, and the authentication string returned from the handset based on, *inter alia,* that RAND sequence (col. 7, lines 46-55).

From the handset number (MIN1), the home CGSA looks up the earlier-established shared secret (SSD) and perform the Jumble operation earlier performed by the handset, *i.e.*, Jumble{RAND+ESN+MIN+SSD.A} to independently compute the authentication string. It compares this with the authentication string received from the local base station and, if they match, the home CGSA forwards the shared secret data (SSD) to the local base station (col. 7, lines 56-68).

By the foregoing registration process, the local base station knows the SSD (and the ESN) of the handset in its service area, and can use this information immediately to validate calls from the handset as they are set-up. In particular, when the handset makes a call, it receives the RAND signal then being broadcast by the local base station, concatenates it with the handset ESN, the shared secret data SSD-A, and the called party's phone number (MIN3), and applies the Jumble procedure. The base station does a parallel operation, and compares the two resulting strings for a match. This operation, and the comparison, are completed quickly (no multi-part exchanges are required), and the base station allows the call to proceed (col. 8, line 61 – col. 9, line 8).

Reed also encrypts the digitized speech transmitted from the handset for further security. In particular, he encrypts the speech using a key produced by applying the Jumble process to {RAND + ESN + MIN1 + SSD-B}. Since the local base station has all this data, it can immediately decrypt the transmitted speech.

In encrypting the speech, it will be recognized that Reed's goal is to achieve security by *preventing access* to the speech by eavesdroppers. He has effectively put the speech intelligence under lock and key, so that only a party with the Jumble-computed key can gain access to it. This is a legitimate theory of security, but it is not the one to which the claimed combinations are directed.

Instead of *preventing access* to speech transmitted by a cell phone, applicant's invention is concerned with *marking* speech transmitted by a cell phone – simply providing a method by which it can be identified. This is a different theory of security.[1]

Consider, as an analogy, a physical article, such as a bicycle. One theory of security says that the bicycle should be kept locked-up, so that only the owner (with the key) can access it. That way it can't get stolen by third party.

A different theory of security says that the bicycle should be labeled with the owner's name and phone number. Others may access it. But because it is marked with the owner's identity, it is unlikely to be stolen by a third party.

Local police often lend metal engraving tools to citizenry for just this purpose – to mark items of value as a deterrent against theft. Attached, as Exhibit A, is a bulletin from the Oregon State University Department of Public Safety, and the Oregon State Police, noting that engravers are available for check-out from a variety of providers, for marking bicycles, stereos, computers, etc., "to help deter theft."

Another relevant example is the current debate about the distribution of electronic music and video files. Should they be distributed with restrictive Digital Rights Management (DRM) provisions - effectively locking them to particular devices on which the content can be played (e.g., only Microsoft's Windows Media Player, or only Apple's iPods)? Or is it preferable for the files to be distributed in a form in which they can be played on all player devices – with unauthorized distribution being deterred by subliminally marking the name of the original owner into the file data (so that content on pirate sharing networks can be traced back to a possible source of the leak)? Both theories have their advantages and disadvantages.

The latter arrangement has been successfully used to mark "screener" videos distributed to members of the Academy of Motion Pictures Arts and Sciences (the voters for the Oscar awards). In 2004, two men were prosecuted for distributing pirated copies of academy screeners. An FBI investigation revealed that actor and Academy voter

---

[1] Of course, encryption can be employed with the presently-claimed arrangements as a further layer of security; however, it does not form part of the claimed arrangements, *per se*.

Carmine Caridi shipped dozens of screener DVDs to a friend. The friend uploaded those movies to file sharing sites, but the files contained watermarks that investigators used to trace their origin back to Caridi. Caridi was expelled from the Academy. (See FBI Press Releases attached as Exhibits B and C.)

Applicant's claims are amended, above, to emphasize the "marking" purpose to which his arrangements are directed.

Turning to the claims, applicant requests reconsideration of the rejections.

As a preliminary matter, applicant does not agree with the premise from which the Office's rejection starts, i.e., that because "*Reeds and Hopper's disclosures are both from the telecommunication field*" that they are properly combinable. This assertion proves too much.

If all telecommunications inventions having antecedents in the telecommunications field were obvious, then essentially nothing in the field of telecommunications would be patentable. It is natural, and proper, that inventors draw from work in their own field.

A more accurate starting point, applicant suggests, is to start with the arguably closest reference, Reeds, and inquire what motivation might an artisan find to alter Reeds (e.g., what shortcoming or deficiency would an artisan recognize). *Then,* based on that motivation, what art would the artisan logically look to?

To start with Reeds and Hopper at the outset - as was done in the present case – unfairly abbreviates the process, and shortchanges the proper role of the hypothetical artisan in the analysis.

As a second ground of traverse, applicant submits that – even starting with Reeds and Hopper – the motivation to combine offered by the Action is illusory.

The Action contends that an artisan would modify Reeds to incorporate Hopper's teachings "because it is desirable for data service to coexist with speech service for various reasons, *i.e., to identify the source of a call.*"

Hopper is not needed for this. Reeds already identifies the source of the call. Reeds' call set-up involves transmission of data based on the handset's electronic serial number (ESN) to the local base station. The base station thus can identify the source of the call. (If it didn't know the ESN of the handset, the base station couldn't validate the call.)

Reeds also identifies the source of the call throughout its duration. As noted in the Action, Reeds encrypts the speech sent to the base station. The encrypted speech is based on the handset's ESN and phone number. Again, the base station's successful decryption of the speech confirms the identity of the source of the call to the base station.

Thus, "to identify the source of a call" is an illusory reason to turn to Hopper's teachings; Reeds already identifies the source of the call.

As a third ground of traverse, applicant respectfully submits that – even if the Action's illusory motivation were pursued - the combination of Reeds and Hopper would not lead to the arrangement claimed.

As noted, the Office proposes that an artisan would have been motivated to employ Hopper's teachings in Reeds "because Hopper discloses that it is desirable for data service to coexist with speech service for various reasons, i.e., to identify the source of a call (col. 1, lines 37-63)."

In the cited passage, Hopper teaches that it is desirable to encode a telephone transmission with the information identifying the caller "*in order to identify the source of annoying or threatening telephone calls.*"

However, an artisan seeking to employ such teaching in Reed would not yield the arrangement of claim 52. In particular, an artisan would not be led to an arrangement in which the "encoding signal" (with which the transmission is marked) "*depends, at least in part, on information received by the radio receiver circuitry and stored in the memory.*"

Hopper teaches that his telephone transmission be marked with an identifier of the caller. Such information is available in Reeds' cell system in the form of the caller's phone number (MIN2 + MIN1), or by the handset's electronic serial number (ESN). Such data is pre-existing in the handset. An artisan following Hopper's teaching – in

Reeds' cell phone – would mark the telephone transmission with one (or both) of these identifiers of the handset. These identifiers were permanently stored in the handset long before its use in the service area of the local base station. No use of "information received by the radio receiver circuitry" would be required.

Thus, if an artisan sought to employ Hopper's teachings so that the source of annoying or threatening telephone calls could be identified, there is no reason that "*information received by the radio receiver circuitry*" would be employed.

Independent claim 55 is similarly non-obvious over the art.

Dependent claim 58 refers to combining an "overlay signal" with the data captured by the data capture system. Applicant did not intend this phrase to have so broad an interpretation as to encompass sidebands resulting from analog modulation, as taught in Hopper. Claim 58 has been amended to make clear that the combination is an *addition* operation (vs. *multiplication* – the signal processing basis for modulation); and that the overlay signal is a digital signal. Hopper does not teach such an arrangement.

Similar amendments have been made to dependent claim 60.

The rejection of independent claim 62 is also traversed.

As with claim 52, the rejection is initially flawed by its immediate identification of Hopper as a combinable reference – without consideration as to the analysis an artisan would actually undertake. That both Hopper and Reeds are in the telecommunications field should not, *per se*, relieve the Office of explaining what would have motivated an artisan, starting from Reeds, to look to Hopper.

A second ground of traverse is that the Hopper art does not teach that for which it is cited.

Claim 62 requires that the steganographic encoder is "adapted to generate an encoding signal that depends – in part – *on dynamics* of the data." Hopper does not teach this.

The Office relies on the fact that Hopper adjusts the amplitude of the data signal so that it does not cause a noticeable distortion in the speech signal (col. 5, lines 3-17). More particularly, Hopper's modulation gain is controlled by a detector (13) that tracks the magnitude of the speech, and controls the gain of the modulation signal (14) accordingly.

This arrangement is not based on dynamics, as recited in claim 62. Instead, it is based on instantaneous scaling. These are different, as explained in applicant's specification at page 10, lines 1-6:

> More satisfactory than basing the instantaneous scaling factor on a single voice data sample, is to base the scaling factor on the dynamics of several samples. That is, a stream of digitized voice data which is changing rapidly can camouflage relatively more auxiliary data than a stream of digitized voice data which is changing slowly. Accordingly, the gain control circuit 50 can be made responsive to the first, or preferably the second- or higher-order derivative of the voice data in setting the scaling factor.

Hopper's disclosure does not contain any teaching of basing a scaling factor on the dynamics of several samples. Hopper's disclosure does not contain any teaching of controlling his variable gain network 14 to be responsive to the first-, second-, or higher-order derivative of the voice information. He does not teach an encoding signal that depends on *dynamics* of the speech information. Thus, even if Hopper's teachings were employed, the arrangement of claim 62 could not result.

(New claims 73 and 74 depend from independent claim 62, and introduce limitations from the just-quoted paragraph.)

Independent claim 65 details a cell phone in which a steganographic encoder is adapted to introduce a pseudo-random signal to the data in which the hidden plural-bit auxiliary code is encoded.

Admittedly, encryption yields pseudo-random signals. However, Hopper does not teach encryption. And Reeds (which *does* employ encryption) does not teach a steganographic encoder.

If Hopper were combined with Reeds (despite the earlier-noted problems with such a starting assumption), there are two ways it might be done. Reeds' speech information could be steganographically encoded before, or after, encryption.

In the former case, steganographic encoding is applied to Reeds' plaintext speech data, and the result is then encrypted.

In the latter case, Reeds' plaintext speech data is first encrypted, and steganographic encoding is then applied to the result.

Claim 65, however, requires that it is the "steganographic encoder" that introduces the pseudo-random signal. In both of the two cases noted above, the pseudo-randomness is introduced not by the steganographic encoding; it is introduced by the encryption.

(Moreover, there is no teaching in Hopper or Reeds that would suggest encrypting the steganographic encoding. Hopper's reason for steganographically encoding the voice transmission is to permit identification of the calling party, e.g., to identify the source of annoying or threatening telephone calls. There is no incentive to prevent access to such identifying information, by encrypting same.)

Thus, even if Hopper and Reeds were combined, the arrangement of claim 65 would not result.

Independent claim 66 is rejected over Reeds in view of Hopper, and further in view of Lee (5,687,191) and Jones (3,586,781).

The Action cites Lee's normalization process (col. 7, lines 34-44) as meeting the claim 66 requirement "the steganographic encoder being adapted to increase certain of the sample value and decrease others."

It appears Lee has been misread. Col. 7, lines 34-44 describe a *prior art* psychoacoustic subband encoder. Such encoders are used in MPEG audio compression systems (i.e., MP3 compressors) to represent audio in more compact fashion. That prior art arrangement does not include any steganographic feature ("hidden data transport" to use Lee's terminology).

In ensuing disclosure, Lee details steganographic arrangements. But, contrary to the rejection, the cited normalization is not performed by Lee's steganographic encoder.

While the foregoing discussion has focused on the independent claims, the dependent claims introduce additional limitations that also contribute to their non-obviousness.

Related Application: 09/924,281

The Examiner's attention is drawn to application 09/924,281, in which the following claims are pending:

1. In a cellular telephone including a microphone, a modulator, an antenna, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, an improvement comprising a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal.

2. The device of claim 1 in which said plural bits comprise data used to discourage piracy of cellular telephony service.

3. The device of claim 1 in which said plural bits comprise data identifying the cellular telephone.

4. A method of operating a cellular telephone, said telephone including a microphone coupled to a transmitter, and a receiver coupled to a transducer, the telephone serving to transmit a wireless signal modulated with a voice signal using an antenna, the method characterized by altering the voice signal to steganographically embed a multi-symbol auxiliary data string therein, wherein transmission of the wireless voice signal also conveys the auxiliary data string hidden therein.

5. In a battery-powered wireless reception device sized for fitting in a user's pocket or purse, the device including an RF amplifier, an antenna, a demodulator, and a speaker, the device serving to receive RF transmissions and output an audio signal conveyed thereby, an improvement comprising a steganographic decoder for discerning multi-symbol auxiliary data conveyed as slight alterations to said audio signal.

6. The device of claim 5 that further includes a processor to which data output by the steganographic decoder is provided.

7. In a method of operating a battery-powered wireless reception device sized for fitting in a user's pocket or purse, the device including an RF amplifier, a demodulator, an antenna, and a speaker, the device serving to receive RF transmissions and output an audio signal conveyed thereby, an improvement comprising steganographically decoding multi-symbol auxiliary data from said audio signal, and controlling some aspect of the device in accordance therewith.

8. A method comprising:

providing a digital information that is to be wirelessly transmitted to a portable device, and at said portable device be rendered in human-perceptible form to a consumer;

steganographically encoding said digital information with plural-bit auxiliary data, prior to being wirelessly transmitted;

at said portable device, recovering said auxiliary data that was steganographically encoded in said digital information;

storing said auxiliary data in said portable device; and

using said stored auxiliary data to control an aspect of the portable device's operation.

9. The method of claim 8 that includes using said stored auxiliary data to reprogram parameters of said portable device.

10. The method of claim 8 that includes transmitting digital information to plural portable devices, wherein each set of said transmitted digital information is steganographically encoded with the same plural-bit auxiliary data.

11. A method comprising:

providing a digital information that is to be wirelessly transmitted to a portable device, and at said portable device be rendered in human-perceptible form to a consumer;

steganographically encoding said digital information with plural-bit auxiliary data, prior to being wirelessly transmitted;

at said portable device, recovering said auxiliary data that was steganographically encoded in said digital information; and

using said auxiliary data to control an aspect of the portable device's operation.

12. The method of claim 11 that includes using said auxiliary data to reprogram parameters of said portable device.

13. The method of claim 11 that includes transmitting digital information to plural portable devices, wherein each set of said transmitted digital information is steganographically encoded with the same plural-bit auxiliary data.

The Examiner in 09/924,281 (Phirin Sam, Art Unit 2616) has allowed claims 8-13, and rejected claims 1-7 over Jensen (5,764,763) in view of Cooperman (5,613,004).

Cooperman is already of record in the present application; an IDS listing Jensen is submitted herewith. (Other art cited in 09/924,281, together with recently noted art, is also listed.)

The substantive contents of the most recent Action in 09/924,281 are reproduced below. Additional documents from that application are available on the online PALM/PAIR file wrapper. Or, if the present Examiner wishes, applicant can submit

copies of other documents from the file. A listing of documents in the 09/479,304 wrapper, copied from PAIR, is also presented below.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,764,763 (hereinafter referred as "Jensen") in view of US Patent 5,613,004 (hereinafter referred as "Cooperman").

Regarding claims 1-3, Jensen discloses in a cellular telephone including a microphone, a modulator, an antenna, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation (see Figs. 1-3, 16, 17, col. 31, lines 59-67, col. 32, lines 1-5, and col. 33, col. 13-29);

Jensen does not disclose a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal. However, Cooperman discloses a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal (see abstract, col. 1, lines 48-57, col. 4, lines 8-27). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the steganographic encoder teaching by Cooperman with Jensen. The motivation for doing so would have been to provide a disincentive to piracy of material read on abstract. Therefore, it would have been obvious to combine Cooperman and Jensen to obtain the invention as specified in the claims 1-3.

Regarding claims 4-7, Jensen discloses a method of operating a cellular telephone, said telephone including a microphone coupled to a transmitter, and a receiver coupled to a transducer, the telephone serving to transmit a wireless signal modulated with a voice signal using an antenna (see Figs. 1-3, 16, 17, col. 31, lines 59-67, col. 32, lines 1-5, and col. 33, col. 13-29);

Jensen does not disclose altering the voice signal to steganographically embed a multi-symbol auxiliary data string therein, wherein transmission of the wireless voice signal also conveys the auxiliary data string hidden therein. However, Cooperman discloses steganographically embed a multi-symbol auxiliary data string and conveys the auxiliary data string hidden (see abstract, col. 1, lines 48-57, col. 4, lines 8-27). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine steganographically embed a multi-symbol auxiliary data string and conveys the auxiliary data string hidden teaching by Cooperman with Jensen. The motivation for doing so would have been to provide a disincentive to piracy of material read on abstract. Therefore, it would have been obvious to combine Cooperman and Jensen to obtain the invention as specified in the claims 4-7.

Allowable Subject Matter

3. Claims 8-13 are allowed.

Response to Arguments

4. Applicant's arguments with respect to claims 1-7 have been considered but are moot in view of the new ground(s) of rejection.

09/924,281 WIRELESS METHODS AND DEVICES EMPLOYING STEGANOGRAPHY

Transaction History

Transaction History

Date	Transaction Description
10-04-2007	Case Docketed to Examiner in GAU
08-21-2007	Mail Non-Final Rejection
08-18-2007	Non-Final Rejection
06-07-2007	Information Disclosure Statement considered
06-07-2007	Reference capture on IDS
06-07-2007	Information Disclosure Statement (IDS) Filed
06-11-2007	Date Forwarded to Examiner
06-07-2007	Response after Non-Final Action
06-07-2007	Information Disclosure Statement (IDS) Filed
04-18-2007	Mail Non-Final Rejection
04-13-2007	Non-Final Rejection
02-15-2007	Information Disclosure Statement considered
02-15-2007	Reference capture on IDS
02-15-2007	Information Disclosure Statement (IDS) Filed
02-15-2007	Information Disclosure Statement (IDS) Filed
02-03-2007	Date Forwarded to Examiner
01-22-2007	Response after Non-Final Action
12-12-2006	Mail Non-Final Rejection
12-11-2006	Non-Final Rejection
10-03-2006	Date Forwarded to Examiner
10-02-2006	Response after Non-Final Action
10-02-2006	Request for Extension of Time - Granted
06-14-2006	Mail Non-Final Rejection
06-12-2006	Non-Final Rejection
04-07-2006	Date Forwarded to Examiner
04-07-2006	Withdrawal of Notice of Allowance
03-22-2006	Mail Notice of Allowance
03-22-2006	Mail Notification of Terminal Disclaimer - Accepted
03-21-2006	Case Docketed to Examiner in GAU
03-20-2006	Notice of Allowance Data Verification Completed
03-20-2006	Case Docketed to Examiner in GAU
03-20-2006	Paralegal TD Accepted
03-20-2006	Notification of Terminal Disclaimer - Accepted
08-07-2001	Terminal Disclaimer Filed
03-16-2006	terminal disclaimer fee paid
03-10-2006	Date Forwarded to Examiner
03-02-2006	Response after Non-Final Action
03-02-2006	Request for Extension of Time - Granted
10-27-2005	Mail Non-Final Rejection
10-26-2005	Non-Final Rejection
07-01-2005	Reference capture on IDS

07-01-2005	Information Disclosure Statement (IDS) Filed
07-01-2005	Information Disclosure Statement (IDS) Filed
07-08-2005	Date Forwarded to Examiner
07-01-2005	Response after Non-Final Action
03-30-2005	Mail Non-Final Rejection
03-28-2005	Non-Final Rejection
03-15-2005	Case Docketed to Examiner in GAU
01-26-2005	Case Docketed to Examiner in GAU
09-22-2004	Case Docketed to Examiner in GAU
07-19-2004	IFW TSS Processing by Tech Center Complete
08-07-2001	Reference capture on IDS
05-19-2004	Miscellaneous Incoming Letter
03-11-2002	Case Docketed to Examiner in GAU
08-07-2001	Information Disclosure Statement (IDS) Filed
08-07-2001	Information Disclosure Statement (IDS) Filed
11-20-2001	Case Docketed to Examiner in GAU
11-03-2001	Application Dispatched from OIPE
11-02-2001	Application Is Now Complete
08-30-2001	Notice Mailed--Application Incomplete--Filing Date Assigned
08-27-2001	Correspondence Address Change
08-21-2001	IFW Scan & PACR Auto Security Review
08-07-2001	Initial Exam Team nn

Applicant called the present application to the attention of Examiner Sam in applicant's last communication in that case, in June 2007.

In the IDS submitted herewith are commonly-owned patents and applications, 6,064,737, 6,278,781 and 20070189533, to which the Examiner's attention is particularly directed in connection with possible double-patenting issues.

The Examiner is invited to telephone the undersigned if it might help bring prosecution of this application to a close.

Respectfully submitted,

Date: October 11, 2007

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

By_____

William Y. Conwell
Registration No. 31,943

Phone: 503-469-4800
FAX 503-469-4777